

### **Amendments to the Claims**

1-3. (Cancelled)

4. (Currently Amended) ~~The cryptographic apparatus of Claim 3, wherein~~ A cryptographic apparatus comprising:

a data reading means for reading content data and cryptographic information from a portable storage medium, the cryptographic information including information used to specify a certain part of the content data on which cryptographic processing is to be performed;

a part specifying means for specifying, based on the read cryptographic information, the certain part of the read content data at least by detecting a specific data section in the read content data; and

a cryptographic processing means for performing one of encryption and decryption on the certain part of the read content data, wherein

a plurality of pieces of content data are each recorded as a file on the storage medium, along with cryptographic information for each of a plurality of file types; and

the data reading means reads, from the storage medium, the content data of a file and the cryptographic information for a corresponding file type,

the cryptographic information includes a reference instruction indicating that a data section in the content data be referred to,

the part specifying means specifies the certain part by referring to the data section as indicated by the reference instruction,

the cryptographic information includes bit pattern information showing a certain bit sequence; and

the part specifying means detects, in the content data, bit data that matches the bit sequence shown in the bit pattern information, and uses a location of the bit data

as a basis for specifying the certain part, the certain part having a fixed positional relationship to the bit data.

5. (Original) The cryptographic apparatus of Claim 4, wherein:  
the indicated data section shows a length of the certain part; and  
the part specifying means specifies the certain part of the content data by referring to the data section as indicated by the reference instruction, and calculating the length of the certain part based on the referenced data section.
6. (Original) The cryptographic apparatus of Claim 5, wherein:  
the cryptographic information includes a value showing a unit used for the indicated data section; and  
the part specifying means specifies the certain part by multiplying the length shown by the data section with the unit value to calculate the length of the certain part.
7. (Previously Presented) The cryptographic apparatus of Claim 6, wherein:  
the cryptographic information further includes a detect instruction for detecting, from the content data, bit data that matches the certain bit sequence shown by the bit pattern information, and specifies the order in which the reference and detect instructions are performed; and  
the part specifying means specifies the certain part in the content data by performing, in the order specified by the cryptographic information, operations indicated by each of the instructions.
- 8-23. (Cancelled)
24. (Currently Amended) ~~The cryptographic apparatus of Claim 19, A cryptographic apparatus encrypting content data and recording the encrypted data onto a storage medium, the cryptographic apparatus comprising:~~

a content data obtaining means for obtaining content data;

a cryptographic information reading means for reading, from a portable storage medium, cryptographic information including information used to specify a certain part of the content data on which cryptographic processing is to be performed;

a part specifying means for specifying the certain part of the obtained content data based on the read cryptographic information at least by detecting a specific data section in the obtained content data;

a cryptographic processing means for encrypting the certain part; and

a content data recording means for recording the encrypted content data onto the storage medium, wherein[[:] ]

the cryptographic information includes bit pattern information showing a certain bit sequence; and

the part specifying means detects, in the content data, bit data that matches the bit sequence shown in the bit pattern information, and uses a location of the bit data as a basis for specifying the certain part, the certain part having a fixed positional relationship to the bit data.

25. (Original) The cryptographic apparatus of Claim 24, wherein:

the cryptographic information includes a reference instruction indicating that a data section in the content data be referred to, the data section showing a length of the certain part; and

the part specifying means specifies the certain part by referring to the data section as indicated by the reference instruction and calculating the length of the certain part based on the referenced data section.

26-30. (Cancelled)

31. (Currently Amended) ~~The cryptographic apparatus of Claim 30, wherein:~~ A  
cryptographic apparatus comprising:  
a data obtaining means for obtaining, from received data, content data, and cryptographic  
information including information used to specify a certain part of the content  
data on which cryptographic processing is to be performed, the received data  
consisting of content data and cryptographic information that has been  
multiplexed and transmitted;  
a part specifying means for specifying the certain part of the obtained content data based  
on the obtained cryptographic information at least by detecting a specific data  
section in the obtained content data; and  
a cryptographic processing means for performing one of encryption and decryption on the  
certain part of the content data; wherein.  
the cryptographic information includes a reference instruction indicating that a data  
section in the content data be referred to,  
the part specifying means specifies the certain part by referring to the data section as  
indicated by the reference instruction,  
the cryptographic information includes sync pattern information showing a certain bit  
sequence; and  
the part specifying means detects, in the content data, a sync pattern corresponding to the  
bit sequence shown in the sync pattern information, and uses a location of the  
sync pattern as a basis for specifying the certain part, the certain part having a  
fixed positional relationship to the sync pattern.
32. (Original) The cryptographic apparatus of Claim 31, wherein:  
the part specifying means verifies the authenticity of the detected sync pattern by  
checking whether another sync pattern is located at a position a set interval away  
from the location of the detected sync pattern.

33. (Previously Presented) The cryptographic apparatus of Claim 31, wherein:
- the cryptographic information further includes flag pattern information showing a bit sequence, which is not the certain bit sequence shown by the sync pattern information, and position information specifying the position of the bit sequence; and
- the part specifying means verifies whether the bit sequence shown by the flag pattern information exists at the position in the content data specified by the position information.
34. (Original) The cryptographic apparatus of Claim 31, wherein:
- the indicated data section shows a length of the certain part; and
- the part specifying means specifies the certain part of the content data by referring to the data section as indicated by the reference instruction, and calculating the length of the certain part based on the referenced data section.
35. (Original) The cryptographic apparatus of Claim 34, wherein:
- the cryptographic information includes a value showing a unit used for the indicated data section; and
- the part specifying means specifies the certain part by multiplying the length shown by the data section with the unit value to calculate the length of the certain part.
36. (Previously Presented) The cryptographic apparatus of Claim 35, wherein:
- the cryptographic information further includes a detect instruction for detecting, from the content data, bit data that matches the certain bit sequence shown by the bit pattern information, and specifies the order in which the reference and detect instructions are performed; and
- the part specifying means specifies the certain part in the content data by performing, in the order specified by the cryptographic information, operations indicated by each of the instructions.

37. (Original) The cryptographic apparatus of Claim 31,  
the cryptographic information further includes at least one piece of algorithm information  
for specifying an algorithm used for cryptographic processing; and  
the cryptographic processing means performs one of encryption and decryption on the  
certain part using the specified algorithm.

38-42. (Cancelled)

43. (Currently Amended) ~~The cryptographic apparatus of Claim 42, wherein:~~ A  
cryptographic apparatus performing cryptographic processing on content data, the  
cryptographic apparatus comprising:  
a content data obtaining means for obtaining content data;  
a cryptographic information obtaining means for obtaining cryptographic information  
including information specifying a part on which cryptographic processing is to  
be performed in the contents data, the information including a reference  
instruction indicating that a data section in the content data be referred to;  
a part specifying means for specifying the certain part of the content data based on the  
cryptographic information by detecting and referring to the data section in the  
content data as indicated by the reference instruction; and  
a cryptographic processing means for performing one of encryption and decryption on the  
certain part, wherein  
the cryptographic information includes bit pattern information showing a certain bit  
sequence; and  
the part specifying means detects, in the content data, bit data that matches the bit  
sequence shown in the bit pattern information, and uses a location of the bit data  
as a basis for specifying the certain part, the certain part having a fixed positional  
relationship to the bit data.

44. (Original) The cryptographic apparatus of Claim 43, wherein:

the cryptographic information includes a reference instruction indicating that a data section in the content data be referred to, the data section showing a length of the certain part; and

the part specifying means specifies the certain part by referring to the data section as indicated by the reference instruction and calculating the length of the certain part based on the referenced data section.

45. (Original) The cryptographic apparatus of Claim 44, wherein:

the cryptographic information includes a value showing a unit used for the indicated data section; and

the part specifying means specifies the certain part by multiplying the length shown by the data section with the unit value to calculate the length of the certain part.

46. (Previously Presented) The cryptographic apparatus of Claim 45, wherein:

the cryptographic information further includes a detect instruction for detecting, from the content data, bit data that matches the certain bit sequence shown by the bit pattern information, and specifies the order in which the reference and detect instructions are performed; and

the part specifying means specifies the certain part in the content data by performing, in the order specified by the cryptographic information, operations indicated by each of the instructions.

47-52. (Cancelled)

53. (Currently Amended) ~~The program recording medium of Claim 51, wherein:~~ A program recording medium storing a control program for having a computer execute cryptographic processing on content data, the control program comprising:

a data reading step for reading content data and cryptographic information from a portable storage medium, the cryptographic information including information used to specify a certain part of the content data on which cryptographic processing is to be performed;

a part specifying step for specifying, based on the read cryptographic information, the certain part of the read content data at least by detecting a specific data section in the read content data; and

a cryptographic processing step for performing one of encryption and decryption on the certain part of the read content data, wherein

the cryptographic information includes bit pattern information showing a certain bit sequence; and

the part specifying step detects, in the content data, bit data that matches the bit sequence shown in the bit pattern information, and uses a location of the bit data as a basis for specifying the certain part, the certain part having a fixed positional relationship to the bit data.

54-59. (Cancelled)

60. (Currently Amended) ~~The program recording medium of Claim 58, wherein:~~ A program recording medium storing a control program for having a computer storing content data execute cryptographic processing on the content data, the cryptographic processing (1) including encryption of the content data and recording of the encrypted content data onto a storage medium, and (2) comprising the following steps:

a cryptographic information reading step for reading, from a portable storage medium, cryptographic information including information used to specify a certain part of the content data on which cryptographic processing is to be performed;

a part specifying step for specifying the certain part of the content data based on the read cryptographic information at least by detecting a specific data section in the content data;



a cryptographic processing step for encrypting the certain part; and  
a content data recording step for recording the encrypted content data onto the other  
storage medium, wherein

the cryptographic information includes bit pattern information showing a certain bit sequence; and

the part specifying step detects, in the content data, bit data that matches the bit sequence shown in the bit pattern information, and uses a location of the bit data as a basis for specifying the certain part, the certain part having a fixed positional relationship to the bit data.

61-62. (Cancelled)

63. (Currently Amended) ~~The program recording medium of Claim 62, wherein:~~ A program recording medium storing a control program for having a computer execute cryptographic processing on content data, the cryptographic processing comprising:

a data obtaining step for obtaining, from received data, content data, and cryptographic information including information used to specify a certain part of the content data on which cryptographic processing is to be performed, the received data consisting of content data and cryptographic information that has been multiplexed and transmitted;

a part specifying step for specifying the certain part of the obtained content data based on the obtained cryptographic information at least by detecting a specific data section in the obtained content data; and

a cryptographic processing step for performing one of encryption and decryption on the certain part of the content data, wherein

the cryptographic information includes sync pattern information showing a certain bit sequence; and

the part specifying step detects, in the content data, a sync pattern corresponding to the bit sequence shown in the sync pattern information, and uses a location of the

sync pattern as a basis for specifying the certain part, the certain part having a fixed positional relationship to the sync pattern.

64. (Original) The program recording medium of Claim 63, wherein:

the part specifying step verifies the authenticity of the detected sync pattern by checking whether another sync pattern is located at a position a set interval away from the location of the detected sync pattern.

65-66. (Cancelled)

67. (Currently Amended) ~~The program recording medium of Claim 66, wherein:~~ A program recording medium storing a control program for having a computer execute cryptographic processing on content data, the cryptographic processing comprising:  
a content data obtaining step for obtaining content data;

a cryptographic information obtaining step for obtaining cryptographic information including information specifying a part on which cryptographic processing is to be performed in the contents data, the information including a reference instruction indicating that a data section in the content data be referred to;

a part specifying step for specifying the certain part of the content data based on the cryptographic information by detecting and referring to the data section in the content data as indicated by the reference instruction; and

a cryptographic processing step for performing one of encryption and decryption on the certain part, wherein

the cryptographic information includes bit pattern information showing a certain bit sequence; and

the part specifying step detects, in the content data, bit data that matches the bit sequence shown in the bit pattern information, and uses a location of the bit data as a basis for specifying the certain part, the certain part having a fixed positional relationship to the bit data.

68. (Original) The program recording medium of Claim 67, wherein:  
the indicated data section shows a length of the certain part; and  
the part specifying step specifies the certain part of the content data by referring to the data section as indicated by the reference instruction, and calculating the length of the certain part based on the referenced data section.

69-72. (Cancelled)

73. (Currently Amended) ~~The data recording medium of Claim 72, wherein:~~ A portable data recording medium storing encrypted content data, the data recording medium comprising:  
a content data recording area in which content data, of which a certain part has been encrypted, is recorded; and  
a cryptographic information recording area in which cryptographic information, including information used to specify the certain part of the content data by detecting a specific data section in the content data, is recorded, wherein  
each of a plurality of pieces of encrypted content data is recorded as a file in the content data recording area; and  
cryptographic information is recorded in the cryptographic information recording area according to file type,  
the cryptographic information includes a reference instruction instructing a decrypting apparatus decrypting the content data to refer to a data section in the content data,  
and  
the cryptographic information includes bit pattern information showing a certain bit sequence, and information instructing the decrypting apparatus to detect, in the content data, bit data matching the certain bit sequence and use a location of the bit data as a basis for specifying the certain part, the certain part having a fixed positional relationship to the bit data.

74. (Original) The data recording medium of Claim 73, wherein  
the indicated data section shows a length of the certain part; and  
the part specifying step specifies the certain part of the content data by referring to the  
data section as indicated by the reference instruction, and calculating the length of  
the certain part based on the referenced data section.

75-76. (Cancelled)

77. (Currently Amended) ~~The data recording medium of Claim 76, wherein:~~ A portable data recording medium storing encrypted content data, the data recording medium comprising:  
a content data recording area in which content data, of which a certain part has been encrypted, is recorded; and  
a cryptographic information recording area in which cryptographic information, including information used to specify the certain part of the content data by detecting a specific data section in the content data, is recorded, wherein  
the cryptographic information includes a reference instruction indicating to a decryption apparatus decrypting the content data that a data section in the content data be referred to,  
the cryptographic information includes bit pattern information showing a certain bit sequence, and  
the cryptographic information further includes a detect instruction for detecting, from the content data, bit data that matches the certain bit sequence shown by the bit pattern information, and specifies the order in which ~~the reference and detect instructions are performed~~ the decryption apparatus performs operations indicated by the reference instruction and the detect instruction.

78-84. (Cancelled)

85. (Previously Presented) A cryptographic apparatus comprising:
- a data reading means for reading content data and cryptographic information from a portable storage medium, the cryptographic information including information used to specify a certain part of the content data on which cryptographic processing is to be performed;
  - a part specifying means for specifying, based on the read cryptographic information, the certain part of the read content data; and
  - a cryptographic processing means for performing one of encryption and decryption on the certain part of the read content data, wherein:
    - the cryptographic information further includes a plurality of pieces of algorithm information for specifying an algorithm used for cryptographic processing, pieces of range information each showing a range over which an algorithm is applied, and information showing priority ratings indicating an order in which the pieces of algorithm information should be applied;
    - the cryptographic processing means selects, for each application range in the certain part, a piece of algorithm information based on the range information, and uses an algorithm specified by the piece of algorithm information to perform one of encryption and decryption on the application range; and
    - when the application ranges of a plurality of algorithms overlap, the cryptographic processing means selects pieces of algorithm information according to the priority ratings.
86. (Previously Presented) A cryptographic apparatus encrypting content data and recording the encrypted data onto a storage medium, the cryptographic apparatus comprising:
- a content data obtaining means for obtaining content data;
  - a cryptographic information reading means for reading, from a portable storage medium, cryptographic information including information used to specify a certain part of the content data on which cryptographic processing is to be performed;

a part specifying means for specifying the certain part of the obtained content data based on the read cryptographic information;

a cryptographic processing means for encrypting the certain part; and

a content data recording means for recording the encrypted content data onto the storage medium, wherein:

the cryptographic information further includes a plurality of pieces of algorithm information for specifying an algorithm used for cryptographic processing, pieces of range information each showing a range in the content data over which an algorithm is applied, and information showing priority ratings indicating an order in which the pieces of algorithm information should be applied;

the cryptographic processing means selects, for each application range in the certain part, a piece of algorithm information based on the range information, and uses an algorithm specified by the piece of algorithm information to encrypt data in the application range; and

when the application ranges of a plurality of algorithms overlap, the cryptographic processing means selects pieces of algorithm information according to the priority ratings.

87. (Previously Presented) A cryptographic apparatus comprising:

a data obtaining means for obtaining, from received data, content data, and cryptographic information including information used to specify a certain part of the content data on which cryptographic processing is to be performed, the received data consisting of content data and cryptographic information that has been multiplexed and transmitted;

a part specifying means for specifying the certain part of the obtained content data based on the obtained cryptographic information; and

a cryptographic processing means for performing one of encryption and decryption on the certain part of the content data, wherein:

the cryptographic information further includes a plurality of pieces of algorithm information for specifying an algorithm used for cryptographic processing, pieces of range information each showing a range over which an algorithm is applied, and information showing priority ratings indicating an order in which the pieces of algorithm information should be applied;

the cryptographic processing means selects, for each application range in the certain part, a piece of algorithm information based on the range information, and uses an algorithm specified by the piece of algorithm information to perform one of encryption and decryption on the application range; and

when the application ranges of a plurality of algorithms overlap, the cryptographic processing means selects pieces of algorithm information according to the priority ratings.

88. (Previously Presented) A cryptographic apparatus performing cryptographic processing on content data, the cryptographic apparatus comprising:

a content data obtaining means for obtaining content data;

a cryptographic information obtaining means for obtaining cryptographic information including information specifying a part on which cryptographic processing is to be performed in the contents data, the information including a reference instruction indicating that a data section in the content data be referred to;

a part specifying means for specifying the certain part of the content data based on the cryptographic information by referring to the data section in the content data as indicated by the reference instruction; and

a cryptographic processing means for performing one of encryption and decryption on the certain part, wherein:

the cryptographic information further includes a plurality of pieces of algorithm information for specifying an algorithm used for cryptographic processing, pieces of range information each showing a range over which an algorithm is applied,

and information showing priority ratings indicating an order in which the pieces of algorithm information should be applied;

the cryptographic processing means selects, for each application range in the certain part, a piece of algorithm information based on the range information, and uses an algorithm specified by the piece of algorithm information to perform one of encryption and decryption on the application range; and

when the application ranges of a plurality of algorithms overlap, the cryptographic processing means selects pieces of algorithm information according to the priority ratings.

89. (Previously Presented) A portable data recording medium storing encrypted content data, the data recording medium comprising:

a content data recording area in which content data, of which a certain part has been encrypted, is recorded; and

a cryptographic information recording area in which cryptographic information, including information used to specify the certain part of the content data, is recorded, wherein:

the cryptographic information further includes a plurality of pieces of algorithm information for specifying an algorithm to be used when decrypting the content data, pieces of range information showing the application range of each piece of algorithm information, and priority ratings used to determine which algorithm information should be applied when the application ranges of a plurality of pieces of algorithm information overlap.